REMARKS

By the present amendment, Claims 1-33 have been amended. Claims 1-33 remain pending in the present application. Claims 1, 6, 15, 19 and 23 are independent claims.

Applicant respectfully submits that the amendments to the claims are fully supported by the original disclosure, and introduce no new matter therewith. Applicant respectfully requests reconsideration and allowance in view of the foregoing amendments and the following remarks.

Applicant appreciates the courtesies extended to Applicant's representative during the personal interview held May 6, 2005. The present response summarizes the substance of the interview. At the interview Applicant's representative discussed a proposed amendment. Proposed amended independent Claim 1 recited method of allowing a user to browse the Web without reducing access and without privacy concerns. The method enabled the user to create a personal profile; accepted a cookie from Web sites of vendors that send cookies; determined if a Web site of a vendor has executed a contract regarding privacy of the personal profile of the user; made available an electronically-created file to the vendor Web site, the file containing or enabling the vendor Web site to access profile information about the user if the vendor Web site has executed the contract regarding privacy of the personal profile of the user; removed or hided the cookie if the vendor Web site has not executed the contract regarding privacy of the personal profile of the user; and forwarded an electronically-created file to the

vendor Web site offering the vendor Web site an opportunity to affirm the contract regarding privacy of the personal profile of the user if the vendor Web site has not executed the contract.

Applicant's representative presented arguments traversing the rejection of Claims 23-33 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter, the rejection of Claims 1-4, 6-21, 23, 24, 26, 27, 31 and 32 under 35 U.S.C. § 103(a) as allegedly being unpatentable over O'Neil et al. (U.S. Patent No. 5,987,440) and Blumenau (U.S. Patent No. US 6,529,952 B1), the rejection of Claims 5, 22 and 33 under 35 U.S.C. § 103(a) as allegedly being unpatentable over O'Neil et al. in view of Blumenau and Merriman et al. (U.S. Patent No. 5,948,061), and the rejection of Claims 25 and 28-30 under 35 U.S.C. § 103(a) as allegedly being unpatentable over O'Neil et al. in view of Blumenau and Rowland et al. (U.S. Patent No. 5,848,412). A formal agreement as to the patentability of the claims was withheld by the Examiner pending a thorough review of arguments and proposed amendment presented at the interview, a thorough review of this amendment, and a further update search.

Claims 23-33 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Applicant respectfully traverses this rejection.

Applicant has amended independent Claim 23 to recite a computer software product having a computer readable medium carrying a computer-executable set of instructions for protecting the privacy of a user. Applicant respectfully submits that amended Claims 23-33 positively recite the computer software product as being

embodied on a tangible medium and are, therefore, now directed to statutory subject matter.

Applicant respectfully requests reconsideration and withdrawal of the rejection of Claims 23-33 under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

Claims 1-4, 6-21, 23, 24, 26, 27, 31 and 32 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over O'Neil et al. (U.S. Patent No. 5,987,440) and Blumenau (U.S. Patent No. US 6,529,952 B1). Applicant respectfully traverses this rejection.

Applicant has revised Claims 1-33 to more particularly define Applicant's claimed invention in view of the prior art of record.

Amended independent Claim 6 recites a method of acting as an intermediary between a user and a vendor Web site. The method enables the user to create a personal profile; accepts a cookie from vender Web sites that send cookies; provides a contract addressing the privacy of the personal profile of the user to the vendor Web site; and causes the contract addressing the privacy of the personal profile of the user to be executed by the vendor Web site.

Amended independent Claims 1, 15, 19 and 23 recite, respectively, a method of allowing a user to browse the Web without reducing access and without privacy concerns, a computerized method of insuring the privacy of a user and obtaining personal information about the user, a system for protecting the privacy of a user, and a computer software product having a computer readable medium carrying a computer-executable set

of instructions for protecting the privacy of a user. Amended independent Claims 1, 15, 19 and 23 set forth the substance of the limitations set forth in amended independent Claim 6, and include additional associated limitations.

The claimed methods, systems, and/or computer program product are related to a network consisting of member users and member vendors and a method of insuring the privacy of those members. The network, known as the e-Privacy Network, allows user members to browse the Web with the security of having a privacy contract (or consent\permission relationship), known as an e-Privacy contract, when browsing the sites of member vendors. Users are protected by cookie-removal protection when browsing a non-member site.

Because user members are protected by an e-Privacy contract, they are confident in submitting or allowing their personally identifiable information, known as an e-profile, to be submitted to member vendors. By protecting personally identifiable information in an e-profile and allowing Web sites to collect non-identifiable information (general information), user members receive better targeted advertisements, offers, deals, etc., as well as incentives for the submission of e-profile information.

When a user of the Web enters a site, the site often sends a cookie, an electronically-created file for tracking a user with a unique identifier for that user. The user may have the option of accepting or refusing the cookie, or the user's browser may automatically accept the cookie (depending on how the browser is set, if it can be adjusted at all). Acceptance of the cookie may be a requirement for uninhibited

browsing, i.e. some sites will not let a user browse or have access without accepting the cookie. The cookie is usually placed on the hard drive of the user's personal computer and retrieved by the site so that it "recognizes" the return of the user. When used with browsing information, i.e. what the user did while on that vendor Web site, a personal profile can be established. Finally, when that user buys something, the vendor Web site knows the personal identity of that user and can equate them with the browsing habits (for its site only) of that user. Many users consider this to be an invasion of privacy.

For example, a user enters a site that sells books, accepts a cookie, and searches for pornographic material. The user leaves the site and returns at some later date (the site recognizes the cookie and knows that the person who earlier searched for pornographic material is back) and buys a mystery book, giving a name and address. The identity is now matched with all of the browsing history and may result in embarrassing mail or other invasions of privacy. It is understandable that users do not want to accept cookies. However, their acceptance may be an inevitable part of searching and browsing Web sites, as noted above.

According to the claimed methods, systems, and/or computer program product, either through e-Privacy software resident on the user's personal computer or on the e-Privacy Web site or any other feasible means, the cookie is accepted. It is then determined if the vendor site is a member of the e-Privacy Network. If the vendor site is a member, the software places a member e-cookie on the hard drive of the user allowing the Web site to collect non-identifiable information (also referred to as general

information) about the user member, and, when required, personal identifiable information about the user, known as the user's e-profile. The invention also contemplates other methods of making available the general information and the personal identifiable information to member vendors, e.g. through forwarding a member e-cookie to the vendor Web site containing or allowing it to collect information.

It is noted that the order of the process is not critical and it can be varied, for example the software may determine if the vendor Web site is a member of the network before the acceptance of the cookie. This order change may allow the software to immediately treat cookies differently depending on their source. If the vendor Web site is not a member of the e-Privacy Network, the cookie sent by the site is removed or hidden after the user completes the session on the site. The non-member site will have information as to the session, for example that the user searched for mystery books, but will not recognize the user when they return because there will be no cookie identifying the user. The non-member vendor Web site may be sent a non-member e-cookie or, alternatively, some type of communication. The non-member e-cookie, which will be generated by the software but will not identify the user to the vendor Web site (there may be user identification means for the e-Privacy Network), will tell the non-member vendor Web site that its cookie has been removed and inform it that its cookies will continue to be removed unless it affirms the e-Privacy contract and joins the e-Privacy Network. The non-member e-cookie may state that their cookie has been returned (without any

identifying information) and invites the non-member vendor Web site to become a member of the e-Privacy Network.

The e-Privacy Network becomes aware of non-member e-cookies sent to non-members so it can follow up if the non-member e-cookies do not result in the non-member joining the network. This awareness will be automatic if the software is resident on its site. If the software is resident on the user's personal computer, messages sent from the software to the network or files that are created by the software and read by the network when the user visits the network site may be ways of notifying the network of non-member e-cookies sent.

Those who affirm the consent/permission relationship (e-privacy contract), either initially and are immediately members of the e-Privacy Network or after receiving a non-member e-cookie, will recognize member vendor Web site e-cookies when a user enters their site. The member vendor Web site e-cookie will enable the vendor Web site to collect non-identifiable information about the user and, when needed, to obtain a user's e-profile information. The member e-cookie includes a means, e.g. a "key", such that when the vendor Web site recognizes the user as a member of the e-privacy network, it will be sent a summary of the e-profile (the Consent profile). This request may occur during the user's session, i.e. in real-time, or at some later time.

After receiving the user's Consent profile, the member vendor Web site may choose to request additional e-profile information. Users are encouraged to respond to these vendor information requests and are often provided incentives to do so by the

vendor Web site member. The response to these requests may be in the form of updating their e-profile information or directly responding to the vendor Web site.

The e-Privacy Network provides confidence to the consumer to accept cookies, or allow the software to accept cookies, and to provide personal information to complete their e-profile. The basis for this confidence is the consent/permission relationship created by the e-Privacy contract. The e-Privacy contract affirms that a vendor Web site will respect the preferences of the user with respect to his personally-identifiable information as summarized in the Consent profile and contained in the e-profile. The terms state that the e-Privacy Network user will see any e-profile information collected about that user (the e-Privacy Network will maintain an audit trail), that the user will from time to time to edit the e-profile information, that the vendor Web site will share this information only with the permission of the user, that the user may "opt out" and the vendor Web site will permanently erase any e-profile information collected, and that the vendor Web site will use reasonable means to protect the security of the e-profile information.

The e-Privacy contract is affirmed by member vendors (this affirmation is a condition of becoming a member), usually by digital certification, and forwarded to the e-Privacy Web site. The e-Privacy Web site updates the list of vendor Web site members based on the receipt of this new contract. Additionally, the e-Privacy software is updated to recognize any new vendor Web sites who join the network. Depending on the location of the software, the software portion of the site is updated or the software on a user's

computer is updated. All Web site members of the e-Privacy Network will be listed and described through the software. Software on the user's computer may be updated the next time that user logs onto the e-Privacy site, either automatically or by making the updated software available for download. The e-Privacy Network may send a notification, e.g. an e-mail, to the user to indicate that new software is available for download.

As discussed above, e-profiles are prepared for delivery to member vendor Web sites with each vendor Web site member receiving a Consent Profile when a user accesses a site, and then receiving the personally-identifiable information according to the preferences of the user member. The user member has previously defined and selected the amount of information that they will allow to be sent to specific vendor Web sites, e.g. the user may choose to provide greater information to sites selling sports-related goods than to sites selling toys. E-profiles are stored on the e-Privacy software, i.e. on the individual user's computer or the e-Privacy site, and are generated by Web-based forms or any other known method for obtaining personal data.

The Examiner states that O'Neil et al. teach substantially all of the features set forth in independent Claims 1, 6, 15, 19, and 23, and concedes that O'Neil et al. does not explicitly teach accepting a cookie from Web sites that send cookies, forwarding an electronically-created file to the site offering the site an opportunity to affirm the contract if the site has not executed the contract, causing the contract to be executed by the Web site, or receiving personal information about the user in exchange for executing the contract. The Examiner then states that Blumenau discloses accepting a cookie from

Web sites that send cookies, forwarding an electronically-created file to the site offering the site an opportunity to affirm the contract if the site has not executed the contract, causing the contract to be executed by the Web site, receiving personal information about the user in exchange for executing the contract. The Examiner then asserts that it would have been obvious to modify the method disclosed by O'Neil et al. as taught by Blumenau to include accepting a cookie from Web sites that send cookies, forwarding an electronically-created file to the site offering the site an opportunity to affirm the contract if the site has not executed the contract, causing the contract to be executed by the Web site, or receiving personal information about the user in exchange for executing the contract.

O'Neil et al. describes a personal information security and exchange tool. The O'Neil et al. invention facilitates the formation and use of networked Trusted Electronic Communities (E-Metro Communities), where each E-Metro Community has several members meeting common admission requirements. The E-Metro Community sets registration rules and verifies member identity itself or facilitates the use of other trusted Certificate Authorities. The informational identity of each member is encapsulated within the E-Metro Community as electronic personal information agents (E-PIAs), with each E-PIA representing a member's information and behavior, with some of the information coming from trusted sources external to the member's E-Metro Community. By establishing and enforcing registration rules and performing accountable and audited verifications of member identity, and if so chosen, personal information certification, the

E-Metro Community builds a community wherein each of its members can belong and participate in an electronic domain where the rights and responsibilities of privacy and informational self-determination are realized. It is through the association and certification by a trusted E-Metro Community that a member becomes trusted and reliable in other transactions, and gains control of their data.

Once a user is a member of an E-Metro Community, the member can assign access rules to each piece of personal information. These access rules set the requirements that must be met before an individual piece of information can be processed. Additionally, the E-Metro Community may get minimum standards for all transactions which must be met. When a request for a particular piece of information is received, E-Metro Community standards and the rule attached to that piece of information is checked by processes specific to the E-Metro Community (E-Metro Community's E-Broker). The E-Broker is the actual process that checks to see if the requester and the situation meet the requirement of the rule. If so, the E-Broker allows the requested information to be processed; if not, the E-Broker does not allow the information to be processed. Additionally, the information may be transport packaged with transitive privilege rules attached that define the requirements for processing by anyone other than the original member. Using these transitive privilege rules, a member can maintain command and control on third party dissemination and processing of their personal information.

A member may also create an agent (E-AutoPIA) to interact with other members in any E-Metro Community, or even data external to any E-Metro Community. This agent contains a subset of the personal information on the member, plus contains an itinerary that directs the activity of the agent. Thus, the agent is able to interact with the personal information of other members as directed in its itinerary.

Blumenau describes a method and system for the collection of cookies and other information from a panel. A panel arrangement is provided to collect access information relating to access by a plurality of panel members of a plurality of web sites. Each of the panel members accesses a corresponding web page stored at a central facility. The web page contains a URL for each of the web sites and an ID uniquely identifying the corresponding panel member. Each panel member transmits, either to each of the web sites corresponding to the URLs of the web page or to the central facility, the ID of the corresponding panel member and any panel member cookies which are stored by the panel member and which correspond to each of at least some of the URLs. Each of the web sites transmits, to the central facility, web site only that access information which relates to the panel members.

Applicant respectfully submits that Blumenau nowhere teaches or reasonably suggests accepting a cookie from vender Web sites that send cookies. The only cookies described by Blumenau are cookies sent from panel members to the Web site that is browsed by users who are statistically represented by the panel members. The panel members go through a screening process before they become panel members. The

cookies the panel members send to the Web site do not include personal profile information about the panel members, they include information regarding surveys they complete as a condition of their becoming panel members. Applicant respectfully submits that modifying O'Neil et al. based on the teachings set forth in Blumenau would destroy the intended function of O'Neil et al.

In order to establish a prima facie case of obviousness, all of the claimed limitations must be taught or suggested by the prior art, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine the reference teachings. *In re Vaek*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). In addition, it is well known that references cannot be combined if the modification destroys the intended function of the reference. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

Applicant respectfully submits that O'Neil et al., Blumenau, or any combination thereof, provides no motivation whatsoever to modify the teachings thereof to provide a method of acting as an intermediary between a user and a vendor Web site, that enables the user to create a personal profile; accepts a cookie from vender Web sites that send cookies; provides a contract addressing the privacy of the personal profile of the user to the vendor Web site; and causes the contract addressing the privacy of the personal profile of the user to be executed by the vendor Web site, as 1-4, 6-21, 23, 24, 26, 27, 31 and 32 require.

Applicant respectfully requests reconsideration and withdrawal of the rejection of Claims 1-4, 6-21, 23, 24, 26, 27, 31 and 32 under 35 U.S.C. § 103(a) as being unpatentable over O'Neil et al. and Blumenau.

Claims 5, 22 and 33 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over O'Neil et al. in view of Blumenau and Merriman et al. (U.S. Patent No. 5,948,061). Applicant respectfully traverses this rejection.

Merriman et al. describes a method of delivery, targeting, and measuring advertising over networks. Statistics are compiled on individual users and networks and the use of the advertisements is tracked to permit targeting of the advertisements of individual users. In response to requests from affiliated sites, an advertising server transmits to people accessing the page of a site an appropriate one of the advertisements based upon profiling of users and networks.

Merriman et al. fails to supplement the deficiencies of O'Neil et al. and Blumenau because Merriman et al. fails to teach or reasonably suggest, and provides no motivation whatsoever to modify the teachings thereof to O'Neil et al., Blumenau, or any combination thereof to provide a method of acting as an intermediary between a user and a vendor Web site, that enables the user to create a personal profile; accepts a cookie from vender Web sites that send cookies; provides a contract addressing the privacy of the personal profile of the user to the vendor Web site; and causes the contract addressing the privacy of the personal profile of the user to be executed by the vendor Web site as set forth in Claims 5, 22 and 33 require.

Applicant respectfully requests reconsideration and withdrawal of the rejection of Claims 5, 22 and 33 are rejected under 35 U.S.C. § 103(a) as being unpatentable over O'Neil et al. in view of Blumenau and Merriman et al.

Claims 25 and 28-30 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over O'Neil et al. in view of Blumenau and Rowland et al. (U.S. Patent No. 5,848,412). Applicant respectfully traverses this rejection.

Rowland et al. describes a user-controlled information disclosure process for web user identification. In this process, a user information database, a BrowserID Client applet, and a BrowserID Website database are configured at a user terminal. The user information database contains a plurality of information records about a users identification information and access levels for the respective information records. The BrowserID Website database contains the names of web sites and access levels for the respective web sites. In response to a request for user information from a web site, the BrowserID Client applet checks the existing access level in the BrowserID Website database for the web site (or negotiates a new level), and if appropriate, retrieves the access key granted by the web site to gain access to a controlled portion of a website.

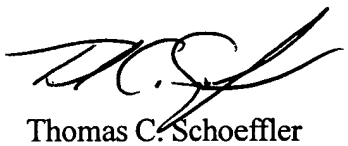
Rowland et al. fails to supplement the deficiencies of O'Neil et al. and Blumenau because Rowland et al. fails to teach or reasonably suggest, and provides no motivation whatsoever to modify the teachings thereof to O'Neil et al., Blumenau, or any combination thereof to provide a method of acting as an intermediary between a user and a vendor Web site, that enables the user to create a personal profile; accepts a cookie

from vender Web sites that send cookies; provides a contract addressing the privacy of the personal profile of the user to the vendor Web site; and causes the contract addressing the privacy of the personal profile of the user to be executed by the vendor Web site as Claims 25 and 28-30 require.

Applicant respectfully requests reconsideration and withdrawal of the rejection of 25 and 28-30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over O'Neil et al. in view of Blumenau and Rowland et al.

For the foregoing reasons, Applicant respectfully submits that the present application is in condition for allowance. If such is not the case, the Examiner is requested to kindly contact the undersigned in an effort to satisfactorily conclude the prosecution of this application.

Respectfully submitted,



Thomas C. Schoeffler
Registration No. 43,385
(703) 486-1000